ENCRYPT

WHITEPAPER 1.0

www.WeAreEncrypt.org

ENCRYPT

Table Of Contents:

ENCRYPT

1. What is ENCRYPT / $XCX ?

ENCRYPT was founded with the mission to make the blockchain arena a more private and decentralized space as was first intended. Many large cryptocurrency/blockchain projects are now opting towards a more intrusive and data collecting setup - this takes away your right to privacy and security. $XCX and ENCRYPT solves this.

Privacy is a right, $XCX makes this possible. Anonymous, untraceable & secure POA/-POS. RingCT, bulletproofs and stealth addresses.

ENCRYPT is the network, $XCX is the cryptocurrency used to transact on the network.

Users will be rewarded additional $XCX for either running a masternode, staking or mining via a blend of POW, POS and POA algorithms.

ENCRYPT

2. History of privacy/security on the blockchain

Blockchain and cryptocurrency was orginally founded with the intention of giving people freedom over their finances. Privacy has been an issue with bitcoin since its inception admist the 2008 market crash. Although transactions may seem private, they can be traced if so wanted as they are only pseudo-anonymous. bitcoin protects some information, but not all. Anyone with a basic understanding of bitcoin can trace the transcation.

The first real projects/coin to tackle this issue was DASH, launched in 2014 and a fork of Bitcoin. DASH utilizes a method called PRIVATESEND of mixing transactions together and introducing them to the blockchain as one single transaction. PRIVATESEND is an implementation of CoinJoin, the privacy solution first proposed for bitcoin by one of the Bitcoin Core developers. Although this is an improvment upon bitcoin, it still isn't truly private. PRIVATESEND is performed via DASH'S masternode system. If a users wants to make their transcation private, they contact a random masternode which collects coins from different users and mixes them together. This means ultimately the user has the trust the masternode wirth their privacy as they can link the sending and receiving addresses.

The more notable coin for privacy is that of MONERO, although its a respected project, it has been proven that its security and privacy is ultimately floored,

ENCRYPT via $XCX will offer next generation privacy for its users via RINGCT, bulletproofs and stealth addr and TX's.

ENCRYPT

3. Coin Specifications

Coin Ticker:	$XCX
Algorithm:	POA / POS
Supply:	10,000,000,000 $XCX
Block Time:	1 Minute
Block Reward:	1000 $XCX
Confirms for spend:	4 Blocks

Emissions per year:	579,036,000 $XCX
Mature Stake time:	100 Blocks
Masternode / Staking split	60/40
Masternode collateral:	500,000 $XCX
Development fund/ Mining	100 $XCX each per block
Premine:	2%

ENCRYPT

4. Chain Specifications

The ENCRYPT network has a number of on chain features that make it amongst the most secure and private cryptocurrencies you can use.

RINGCT:

RingCT works by taking a user's transaction and mixing it with a number of other outputs from the blockchain network. These outputs are added together in a way that makes them identical, meaning any one of the outputs could plausibly be the real transaction. Next up, a key image is added to the transaction to prevent users from double spending. The miners on the network have a list of every key image ever used, so if the same one pops up, that transaction is ignored.

By building a network that has cryptographically sound privacy mechanisms into every part of the transaction, users can interact with privacy-focused dApps without needing to understand how it works. Simply put, RingCT makes transactions untraceable and unlinkable. As the crypto space moves to a more decentralized model, having a project that is focused on privacy dApps can create an entire private, decentralized economy.

$XCX will implement however a set string range of 6-12. Morero and others only use a setring of 11. A range makes the transcation even more secure.

BULLETPROOFS:

Bulletproofs are short non-interactive zero-knowledge proofs that require no trusted setup. A bulletproof can be used to convince a verifier that an encrypted plaintext is well formed. For example, prove that an encrypted number is in a given range, without revealing anything else about the number. Compared to SNARKs, Bulletproofs require no trusted setup. However, verifying a bulletproof is more time consuming than verifying a SNARK proof.

Bulletproofs are designed to enable efficient confidential transactions in Bitcoin and other cryptocurrencies. Confidential transactions hide the amount that is transfered in the transaction. Every confidential transaction contains a cryptographic proof that the transaction is valid. Bulletproofs shrink the size of the cryptographic proof from over 10kB to less than 1kB. Moreover, bulletproofs support proof aggregation, so that proving that m transaction values are valid adds only O(log(m)) additional elements to the size of a single proof. If all Bitcoin transactions were confidential and used Bulletproofs, then the total size of the UTXO set would be only 17 GB, compared to 160 GB with the currently used proofs.

Bulletproofs have many other applications in cryptographic protocols, such as shortening proofs of solvency, short verifiable shuffles, confidential smart contracts, and as a general drop-in replacement for Sigma-protocols.

ENCRYPT

4. Chain Specifications

STEALTH ADDRESSES / STEALTH TRANSACTIONS

Stealth addresses are designed to prevent public association of a transaction's output with a recipient's wallet address and conceal a transaction's actual destination address, thereby hiding the receiver's identity on a cryptocurrency network.

Stealth addresses are a technique for obscuring public blockchain transactions.
A core property of blockchain is pseudonymous transactions, which means once personal information, like an IP address, is associated with a crypto key, all the transactions using that key can be traced on the blockchain.
Stealth addresses are private, single-use addresses generated using the elliptic-curve Diffie-Hellman protocol.

ENCRYPT

5. Roadmap

Our roadmap will be an ever developing concern. It will be community driven and open source. ENCRYPT founders have outlined the intital path.

ENCRYPT

7. Team

The ENCRYPT team consists of a cluster of high level developers, at this time they will remain anonymous.

ENCRYPT

7. Sources:

https://www.investopedia.com/terms/s/stealth-address-cryptocurrency.asp

https://hackernoon.com/blockchain-network-using-bitcoin-code-base-adds-ringct-and-bulletproofs-g21lw38h6

https://crypto.stanford.edu/bulletproofs/